REMARKS

Claims 1 – 31 are pending in the application. Claims 1, 5, 9, 13-14 and 21 are amended in this response.

Claim Rejections – 35 USC 103

Claims 1 – 8, 13 – 16, and 21 - 27 were rejected under 35 USC 103(a) as being unpatentable over the article by Jung, in view of Shefi US 6,266,413, and further in view of Maurer US 5,253,294.

The Examiner further rejected claims 9-12,17-20, and 28-31 under 35 USC 103(a) as being unpatentable over Jung, Shefi and Maurer, in further view of Midgley et al, US Patent No. 6,460,055.

Favorable reconsideration of this rejection in view of the following explanations is respectfully requested.

The present invention, as described in the Field of the Invention section, relates to a method and an apparatus for the provision of random data for the use of secret communication, and more particularly but not exclusively to a practical method and apparatus for providing identical random data in a confidential manner to parties connected via an open network, where the random source is publicly available on the network, see the amended preambles to the independent claims.

The present claims define a novel and inventive method for providing identical and ***regularly changing*** random data at two or more separate locations. The random data has a single source, which ***is external*** to the two parties and may be accessible to **anyone**. Nevertheless, the method provides confidentially to each of the locations in such a way that it is not available to eavesdroppers, as a result of using an

identical selector deployed at each of the parties. Each of the identical selectors selects at the respective party the ***same*** random bit source from the single regularly changing external source,.

The prior art citations fail either singly or in combination to teach regularly changing identical random sources at two different locations based on a single generally available and regularly changing random source. In particular, all of the citations teach that the source is secret, and thus there is no combination of the prior art that can teach all the features of the newly amended claim.

Considering the references one by one, the Shefi system provides a completely different solution. With the Shefi system, two parties share a ***secret source*** – a large table of random numbers, or several such tables. This commonly held secret source further differs from the source of the claimed invention in that Shefi's source is fixed and does not change over time nor over the course of the communication. To start a process between the two parties in Shefi they send to each other a pointer to a starting position in the table. The starting pointer is sent in the ***open, not in secret, but this does not matter as it is supposed that the table to which it refers is secret***. The pointer is then used to move along the same fixed secret table at both parties. That is to say, the pointer starting tuning is not secret, and a third party can also obtain the starting pointer by eavesdropping. The secrecy is supposed to be achieved by the **secrecy of the *secret source,*** the **fixed** large table of random number that both parties have and **no third party has**. However the disadvantage with Shefi is that the table(s) are fixed over the long term and, should a third party somehow obtain this large table(s), perhaps even by bribing or like means, the whole system becomes available to him. Typically he has plenty of time to use this fixed secret table(s) as the transmissions include the non-secret transmitted pointers which will allow him to

synchronise. This problem is solved by the presently claimed invention since the random source changes regularly, and preferably continuously. There is thus no leakage of information that would be valuable for any length of time.

Jung describes a CFB-mode of encryption. The CFB-mode of encryption is well known and has been used for a long time, indeed for many decades, and is written and explained in almost any basic textbook of cryptography.

With CFB-mode encryption, the ciphertext is **copied**, not selected in ***serial order of appearance*** **as a whole** into the register, generally byte by byte, and the register is shifted. The output of the register is processed serially using a fixed **secret key** by a block cipher algorithm to output a stream of bits for XOR-ing the stream with the plaintext. With Jung, the **only secret element** is the fixed **secret key** and **no selection** whatsoever occurs. Once a third party gets hold, either by cryptanalysis or through bribery and the like, of the **fixed secret key** the whole system is open for the long term, a problem that does not arise with the claimed invention as all the key information changes regularly, as explained above.

The Maurer patent, newly cited in the present Office Action, follows the approach and principal of Shefi, of course with differences between them in details and practice. The Maurer system, as with the Shefi one, requires a secret source. With the Maurer system, two parties share a ***secret source*** –with the Maurer system, the source is a large fixed secret **library** of random numbers, as opposed to a table. To start a process between the two parties they send to each other a starting pointer, or in Maurer's words, a key index signal. The starting pointer is sent in the ***open, not in secret.*** To quote from the Abstract: "The key index signal, which is transmitted to all stations that must decrypt the message signal and therefore subject to interception…", and it can be understood also from the description of the Maurer invention. This

pointer is then used to select from the same **secret** fixed library at both parties. That is to say, the pointer (starting) tuning is not secret, and a third party can also obtain the pointer. The secrecy is supposed to be achieved by the **secrecy of the *secret source, the*** large fixed library of random numbers that both parties have and **no third party has**. As stated in Maurer, page 9, lines 3-13: "The only transmitted signal subject to intruder interception besides the cipher text is a random number needed to select the day key and initialize the PRNGs. Armed with this information and even an identical terminal, but absent the specific key library memories, there is no known way in which an intruder can recover the contents of the memories in any reasonable time period and therefore break the code. Memories may thus be produced in secret and be changed only very infrequently with no fear of loss of security".

Turning now to the present application, claim 1 defines a system for sharing a random process between at least two separate parties, the system comprising at each party: a copy of a part of a primary digital bitstream, the primary digital stream being *located externally* to the at least two separate parties, and is not fixed but rather dynamically changes over a session, that is during communication between the parties. A copy of the source is available at the separate parties, and a selector is used to randomly select a part of the primary digital bitstream to form a random bit source. Each selector in fact then uses the random bit source itself to randomize the selection operation in an identical manner at each separate party, thereby to render the random bit source available at respective ones of the separate parties.

The present invention, as defined by claim 1, teaches a system which uses a copy of an *external* and *available* primary digital bitstream, a stream which is not fixed but dynamically changes and develops during the course of time and during the

course of the communication, and includes a selector which selects parts of the copy of the *external* primary digital bitstream to form a random bit source.

That is to say, with the present invention, the random data has a single source, which is not fixed but dynamically changes and develops during the course of communication between the parties and which *is external* to the two parties, and is typically accessible to anyone.

For example, the present disclosure teaches on page 21, line 7: "Thus, the processes described above may rely on any source of highly shuffled data including external sources, and need not require any initial arrangement of the data in order to use the data in real time operation".

By contrast, the Shefi and Maurer systems provide a totally opposite solution. With the Shefi and the Maurer systems, two parties share a *secret source* – a large fixed table of random number (or several such tables) for the Shefi case and a large fixed library of random number for the Maurer case. That is to say, with Shefi and Maurer, the primary digital bitstream is secret and internal to the participating parties only and is fixed over the course of the communication. On the other hand the starting pointer, used for pointing at a starting position at the secret table or library, and generating a random bit stream may be revealed to the public as it is sent from the parties to each other in the open.

For example, Shefi describes in column 10, line 22: "The system includes an electronic device, for example a semiconductor chip, which contains at least one table of random numbers, and which is able to generate an electronic "one-time pad". In order for secure communication to take place, each party must have this chip or another form of the electronic device of the present invention. Any two parties having

the electronic device of the present invention can then communicate securely or perform a secure identification procedure."

Shefi further describes in column 10, line 30: "In either case, the two parties preferably send at least one random number to each other as part of the key. The key is then used as part of the method of the present invention for generating an electronic "one-time pad" by selecting at least one true random number from a table of true random numbers according to a selection procedure."

Neither Shefi nor Maurer ever describe or even hint at the idea of a system using an *external* **changing** primary digital bitstream, or a randomly changing secret selection as defined by claim 1 and the other independent claims.
Maurer is quoted above.

As described hereinabove, Jung also fails to describe or even hint at the idea of a system using an *external* primary digital bitstream, with a randomly changing secret selection as taught by the present invention, and defined by claim 1. With Jung, the *only secret element is the* **fixed** *secret key* and *no (secret) selection* whatsoever occurs.

For example, Jung describes on page 344, in section 3.1: "In a standard case, n bits of the ciphertext are fed back into the shift register, i.e. if n bits of generated key steam are used for the encryption of n bits of plaintext."
Thus Shefi or Maurer combined with Jung also falls short of teaching the idea of a system using an *external* **changing** primary digital bitstream, or a randomly changed secret selection as taught by the present invention, and defined by claim 1. None of these documents teaches in any combination an available *regularly changing* primary *random* source.

It is thus respectfully believed that claim 1 as amended is novel and inventive over both Jung, Shefi and Maurer, and the combination thereof, and should be allowed.

Claim 13, defines a random data generator for sharing a random process between at least two separate parties in secret manner based on a publicly available primary digital bitstream, the generator comprising:

an input configured for receiving at regular intervals a copy of a current part of said available digital bitstream, said available digital bit stream being located externally to parties using the generator,

a random selector for selecting random individual bits from said available digital bitstream to form said current part, said current part thus comprising a random data stream that is changed regularly,

wherein said random selector is randomized by a previous segment of said regularly changing random data stream, such as to allow said regularly changing random data stream to be available at any location at which said digital bitstream is available.

Claim 13 as amended and explained hereinabove, teaches a random data generator which uses a copy of an *external* **changing** digital bitstream, and includes a random selector for randomly selecting parts of the copy of the *external* digital bitstream to form a random bit source.

That is to say, with the present invention, the random data has a single **changing** source, which *is external* to the two parties, and an inherent randomly changed random secret selector.

As explained in further detail hereinabove, the citations of Jung, Shefi and Maurer fail to teach even in combination idea of a random data generator using a copy of an *external* **changing** ***and generally available*** digital bitstream, nor an inherent

randomly changing random secret selector as taught by the present invention, and defined by claim 13.

It is thus respectfully believed that claim 13 is novel and inventive over both Jung Shefi and Maurer and should be allowed.

Claim 14, defines A random data generator for reproducing a random data stream producible by an identical generator at another location for sharing a random process between at least two separate parties in secret manner, based on a publicly available primary digital bitstream, comprising:

an input configured for regularly receiving a current copy of a part of said available digital bitstream, said available digital bitstream being available in identical manner at a plurality of locations, said available digital bit stream being external to the locations,

a random selector configured for selecting said part, said part comprising random individual bits from said available regularly changing digital bitstream, therefrom to form a regularly changing random data stream,

wherein said random selector is randomized by a previous part of said regularly changing random data stream, thereby to enable said random data stream to be available in identical manner at a plurality of locations.

The present invention, as defined by claim 14 and explained hereinabove, teaches a random data generator which uses a copy of an *external* regularly **changing** digital bitstream, and includes a random selector for randomly selecting parts of the copy of the *external* digital regularly changing bitstream to form a random bit source.

That is to say, with the present invention, the random data has a single **changing** source, which *is external* to the two parties and an inherent randomly changed random secret selector.

As explained in further detail hereinabove, neither Jung nor Shefi nor Maurer, whether taken alone or in combination, teaches or even hints at the idea of a random data generator using a copy of a **changing** *external* digital bitstream, nor an inherent randomly changed random secret selector as taught by the present invention, and defined by claim 14.

Claim 21, defines a method for secret sharing of a random process between at least two separate parties based on a publicly available source, comprising the steps of:

randomly selecting at each party in a selection operation a regularly changing copy of a part of an available and regularly changing primary digital data bit stream, said available primary digital data bit stream being external to the parties and available in identical manner at each party, said randomly selected regularly changing copy to form a regularly changing random data source changing identically at each party, and

using said regularly changing random data source to randomize said selection operation in an identical manner at each party, thereby to render said random process available in identical manner at each party.

That is to say, with the present invention, the random data has a single **changing** source, which *is external* to the two parties and an inherent randomly changing random secret selector.

As explained in further detail hereinabove, neither Jung nor Shefi nor Maurer teaches or even hints at, either alone or in combination, the idea of a method using a copy of

an *external* **changing** digital bitstream, or an inherent randomly changed random secret selector as defined by claim 21.

The remaining claims mentioned in this section of the Office Action are believed to be allowable as being dependent on an allowable main claim.

All of the matters raised by the Examiner have been dealt with and are believed to have been overcome.

In view of the foregoing, it is respectfully submitted that all the claims now pending in the application are allowable.

An early Notice of Allowance is therefore respectfully requested.

Respectfully submitted,

Martin D. Moynihan

Martin D. Moynihan
Registration No. 40,338

Date: June 7, 2007

Encls:

- Petition for Extension for Three (3) Months Time
- Request for Continued Examination (RCE)